PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2003-298565
(43)Date of publication of application : 17.10.2003

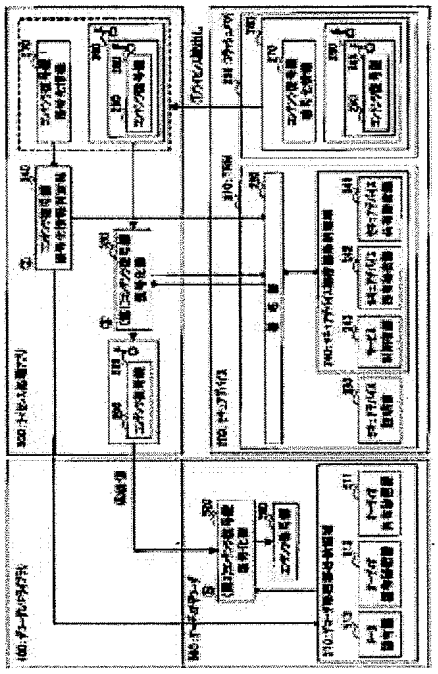
(51)Int.Cl. H04L 9/08
G06F 12/14
G11B 20/10
H04L 9/10
H04L 9/14

(21)Application number : 2002-098038
(22)Date of filing : 29.03.2002

(71)Applicant : MATSUSHITA ELECTRIC IND CO LTD
(72)Inventor : FURUYAMA JUNKO
MINEMURA ATSUSHI

(54) CONTENTS DISTRIBUTION SYSTEM

(57)Abstract:
PROBLEM TO BE SOLVED: To provide a contents distribution system for performing diversified contents distribution services within the same framework.
SOLUTION: A TRM (Tamper Resistant Module) 210 of a secure device 200 stores a plurality of secret keys (secure device share secret key 241, secure device unique secret key 242, and service user key 243), a decoder 500 stores a plurality of secret keys (audio share secret key 511, audio unique secret key 512, manufacture unique key 513), and a server 100 encrypts the decoding key 290 of encrypted contents by using a public key of the secure device 200 and a public key of the decoder 500 in duplicate depending on the contents distribution service.



(19)日本国特許庁（ＪＰ）　(12)**公開特許公報**（Ａ）　(11)特許出願公開番号
特開2003－298565
（P2003－298565A）
(43)公開日　平成15年10月17日(2003.10.17)

(51)Int.Cl.[7]	識別記号	ＦＩ		テーマコード（参考）
Ｈ０４Ｌ　9/08		Ｃ０６Ｆ　12/14	３２０Ｂ	５Ｂ０１７
Ｇ０６Ｆ　12/14	３２０	Ｃ１１Ｂ　20/10	Ｄ	５Ｄ０４４
Ｇ１１Ｂ　20/10			Ｈ	５Ｊ１０４
		Ｈ０４Ｌ　9/00	６０１Ｂ	
Ｈ０４Ｌ　9/10			６４１	

審査請求　未請求　請求項の数18　ＯＬ　（全 12 頁）　最終頁に続く

(21)出願番号　特願2002－98038(P2002－98038)

(22)出願日　平成14年３月29日(2002.3.29)

(71)出願人　000005821
松下電器産業株式会社
大阪府門真市大字門真1006番地

(72)発明者　古山　純子
大阪府門真市大字門真1006番地　松下電器産業株式会社内

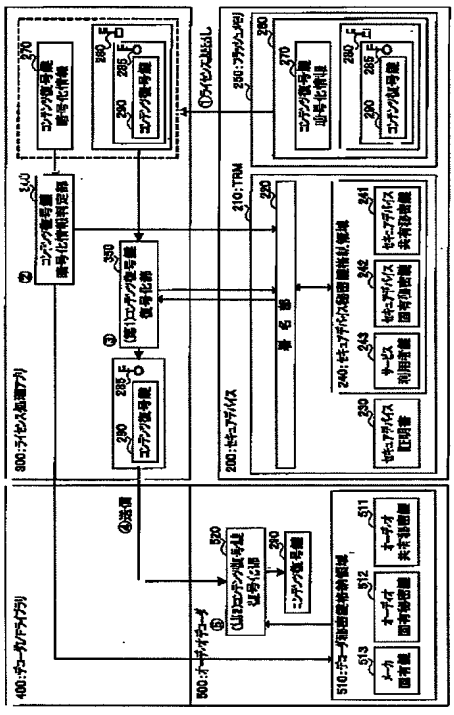
(72)発明者　峰村　淳
大阪府門真市大字門真1006番地　松下電器産業株式会社内

(74)代理人　100105050
弁理士　鷲田　公一

最終頁に続く

(54)【発明の名称】　コンテンツ配信システム

(57)【要約】
【課題】　同じ枠組みでコンテンツ配信のいろいろなサービスを行うこと。
【解決手段】　セキュアデバイス２００のＴＲＭ２１０内に複数の秘密鍵（セキュアデバイス共有秘密鍵２４１、セキュアデバイス固有秘密鍵２４２、サービス利用者鍵２４３）を格納するとともにデコーダ５００に複数の秘密鍵（オーディオ共有秘密鍵５１１、オーディオ固有秘密鍵５１２、メーカ固有鍵５１３）を格納しておき、サーバ１００で、コンテンツ配信サービスに応じて、暗号化コンテンツの復号鍵２９０をセキュアデバイス２００の公開鍵とデコーダ５００の公開鍵とで二重に暗号化する。



【特許請求の範囲】
【請求項１】　コンテンツを配信するサーバ装置と、前記サーバ装置によって配信されたコンテンツを記録する記録媒体装置と、前記記録媒体装置に記録されたコンテンツを再生する再生装置とを有するコンテンツ配信システムであって、
前記記録媒体装置は、
複数の記録媒体装置用の鍵を記憶する第１記憶手段、を有し、
前記再生装置は、
複数の再生装置用の鍵を記憶する第２記憶手段、を有し、
前記サーバ装置は、
前記第１記憶手段に記憶された複数の記録媒体装置用の鍵とおのおの対をなす複数の記録媒体装置用の鍵および前記第２記憶手段に記憶された複数の再生装置用の鍵とおのおの対をなす複数の再生装置用の鍵の中からそれぞれ１つの記録媒体装置用の鍵および再生装置用の鍵を取得する取得手段と、
前記取得手段によって取得された記録媒体装置用の鍵および再生装置用の鍵を用いて、暗号化されたコンテンツを復号化するための暗号化コンテンツ復号鍵を二重に暗号化する暗号化手段と、
を有することを特徴とするコンテンツ配信システム。
【請求項２】　前記第１記憶手段に記憶された複数の記録媒体装置用の鍵は、全部の記録媒体装置に共有の全共有鍵と、各記録媒体装置に固有の固有鍵とを含むことを特徴とする請求項１記載のコンテンツ配信システム。
【請求項３】　前記第１記憶手段に記憶された複数の記録媒体装置用の鍵は、全部の記録媒体装置に共有の全共有鍵と、特定の範囲の記録媒体装置に共有の特定範囲共有鍵とを含むことを特徴とする請求項１記載のコンテンツ配信システム。
【請求項４】　前記第１記憶手段に記憶された複数の記録媒体装置用の鍵は、各記録媒体装置に固有の固有鍵と、特定の範囲の記録媒体装置に共有の特定範囲共有鍵とを含むことを特徴とする請求項１記載のコンテンツ配信システム。
【請求項５】　前記第１記憶手段に記憶された複数の記録媒体装置用の鍵は、全部の記録媒体装置に共有の全共有鍵と、各記録媒体装置に固有の固有鍵と、特定の範囲の記録媒体装置に共有の特定範囲共有鍵とを含むことを特徴とする請求項１記載のコンテンツ配信システム。
【請求項６】　前記第２記憶手段に記憶された複数の再生装置用の鍵は、全部の再生装置に共有の全共有鍵と、各再生装置に固有の固有鍵とを含むことを特徴とする請求項１記載のコンテンツ配信システム。
【請求項７】　前記第２記憶手段に記憶された複数の再生装置用の鍵は、全部の再生装置に共有の全共有鍵と、特定の範囲の再生装置に共有の特定範囲共有鍵とを含むことを特徴とする請求項１記載のコンテンツ配信システム。
【請求項８】　前記第２記憶手段に記憶された複数の再生装置用の鍵は、各再生装置に固有の固有鍵と、特定の範囲の再生装置に共有の特定範囲共有鍵とを含むことを特徴とする請求項１記載のコンテンツ配信システム。
【請求項９】　前記第２記憶手段に記憶された複数の再生装置用の鍵は、全部の再生装置に共有の全共有鍵と、各再生装置に固有の固有鍵と、特定の範囲の再生装置に共有の特定範囲共有鍵とを含むことを特徴とする請求項１記載のコンテンツ配信システム。
【請求項１０】　前記サーバ装置は、
暗号化コンテンツ復号鍵を二重に暗号化する際に使用する記録媒体装置用の鍵および再生装置用の鍵を、コンテンツ配信サービスに応じて決定する決定手段、をさらに有し、
前記取得手段は、
前記決定手段の決定結果に従って、前記第１記憶手段に記憶された複数の記録媒体装置用の鍵とおのおの対をなす複数の記録媒体装置用の鍵および前記第２記憶手段に記憶された複数の再生装置用の鍵とおのおの対をなす複数の再生装置用の鍵の中からそれぞれ１つの記録媒体装置用の鍵および再生装置用の鍵を取得する、
ことを特徴とする請求項１記載のコンテンツ配信システム。
【請求項１１】　前記サーバ装置は、
前記暗号化手段によって二重に暗号化された暗号化コンテンツ復号鍵ならびに当該暗号化コンテンツ復号鍵を二重に暗号化する際に使用した記録媒体装置用の鍵および再生装置用の鍵に関する暗号化コンテンツ復号鍵暗号化情報を配信する配信手段、
をさらに有することを特徴とする請求項１記載のコンテンツ配信システム。
【請求項１２】　コンテンツを配信するサーバ装置と、前記サーバ装置によって配信されたコンテンツを記録する記録媒体装置と、前記記録媒体装置に記録されたコンテンツを再生する再生装置とを有するコンテンツ配信システムにおけるバインド方式制御方法であって、
前記サーバ装置が、前記記録媒体装置に記憶された複数の記録媒体装置用の鍵とおのおの対をなす複数の記録媒体装置用の鍵および前記再生装置に記憶された複数の再生装置用の鍵とおのおの対をなす複数の再生装置用の鍵の中からそれぞれ１つの記録媒体装置用の鍵および再生装置用の鍵を取得する取得ステップと、
前記サーバ装置が、前記取得ステップで取得した記録媒体装置用の鍵および再生装置用の鍵を用いて、暗号化されたコンテンツを復号化するための暗号化コンテンツ復号鍵を二重に暗号化する暗号化ステップと、
を有することを特徴とするコンテンツ配信システムにおけるバインド方式制御方法。

【請求項１３】　コンテンツを配信するサーバ装置であって、
前記サーバ装置によって配信されたコンテンツを記録する記録媒体装置に記憶された複数の記録媒体装置用の鍵とおのおの対をなす複数の記録媒体装置の鍵および前記記録媒体装置に記録されたコンテンツを再生する再生装置に記憶された複数の再生装置用の鍵とおのおの対をなす複数の再生装置用の鍵の中からそれぞれ１つの記録媒体装置用の鍵および再生装置用の鍵を取得する取得手段と、
前記取得手段によって取得された記録媒体装置用の鍵および再生装置用の鍵を用いて、暗号化されたコンテンツを復号化するための暗号化コンテンツ復号鍵を二重に暗号化する暗号化手段と、
を有することを特徴とするサーバ装置。
【請求項１４】　コンテンツを配信するサーバ装置におけるバインド方式制御方法であって、
前記サーバ装置によって配信されたコンテンツを記録する記録媒体装置に記憶された複数の記録媒体装置用の鍵とおのおの対をなす複数の記録媒体装置用の鍵および前記記録媒体装置に記録されたコンテンツを再生する再生装置に記憶された複数の再生装置用の鍵とおのおの対をなす複数の再生装置用の鍵の中からそれぞれ１つの記録媒体装置用の鍵および再生装置用の鍵を取得する取得ステップと、
前記取得ステップで取得した記録媒体装置用の鍵および再生装置用の鍵を用いて、暗号化されたコンテンツを復号化するための暗号化コンテンツ復号鍵を二重に暗号化する暗号化ステップと、
を有することを特徴とするサーバ装置におけるバインド方式制御方法。
【請求項１５】　コンテンツを配信するサーバ装置におけるバインド方式制御プログラムであって、
前記サーバ装置によって配信されたコンテンツを記録する記録媒体装置に記憶された複数の記録媒体装置用の鍵とおのおの対をなす複数の記録媒体装置用の鍵および前記記録媒体装置に記録されたコンテンツを再生する再生装置に記憶された複数の再生装置用の鍵とおのおの対をなす複数の再生装置用の鍵の中からそれぞれ１つの記録媒体装置用の鍵および再生装置用の鍵を取得する取得ステップと、
前記取得ステップで取得した記録媒体装置用の鍵および再生装置用の鍵を用いて、暗号化されたコンテンツを復号化するための暗号化コンテンツ復号鍵を二重に暗号化する暗号化ステップと、
をコンピュータに実行させることを特徴とするサーバ装置におけるバインド方式制御プログラム。
【請求項１６】　サーバ装置によって配信されたコンテンツを記録する記録媒体装置であって、
複数の記録媒体装置用の鍵を記憶する第１記憶手段、
を有することを特徴とする記録媒体装置。
【請求項１７】　サーバ装置によって配信され記録媒体装置に記録されたコンテンツを再生する再生装置であって、
複数の再生装置用の鍵を記憶する第２記憶手段、
を有することを特徴とする再生装置。
【請求項１８】　コンテンツを配信するサーバ装置と、前記サーバ装置によって配信されたコンテンツを記録する記録媒体装置と、前記記録媒体装置に記録されたコンテンツを再生する再生装置とを有するコンテンツ配信システムであって、
前記記録媒体装置は、
複数の記録媒体装置用の鍵を記憶する第１記憶手段、を有し、
前記再生装置は、
複数の再生装置用の鍵を記憶する第２記憶手段、を有し、
前記サーバ装置は、
前記第１記憶手段に記憶された複数の記録媒体装置用の鍵とおのおの対をなす複数の記録媒体装置用の鍵および前記第２記憶手段に記憶された複数の再生装置用の鍵とおのおの対をなす複数の再生装置用の鍵の中からそれぞれ１つの記録媒体装置用の鍵および再生装置用の鍵を取得する取得手段と、
前記取得手段によって取得された記録媒体装置用の鍵および再生装置用の鍵を用いて、配信するコンテンツを二重に暗号化する暗号化手段と、
を有することを特徴とするコンテンツ配信システム。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】本発明は、コンテンツ配信システムに関する。
【０００２】
【従来の技術】近年、デジタル化された文書や音楽、映像、プログラム、電子チケットなどのコンテンツがインターネットなどのネットワークを経由して流通し、ユーザは、所望のコンテンツを簡単にネットワークを経由して取り出し、記録媒体（メディア）に記録し、再生することができるようになってきている。
【０００３】たとえば、従来のコンテンツ配信システムでは、サーバから、暗号化されたコンテンツやユーザ固有鍵で暗号化されたコンテンツ復号鍵を端末に配信してこの端末の記録媒体に記録し、そして、この端末で、コンテンツ復号鍵の復号化や、コンテンツのライセンスの検証・更新などの処理を行ってコンテンツを再生することが行われていた。このとき、端末では、コンテンツの利用制御をセキュアに行うために、セキュアＬＳＩやＴＲＭ（Tamper Resistant Module：耐タンパモジュール）などを使用する場合が多い。
【０００４】また、その際、コンテンツ再生に使用され

る端末は、コンテンツ配信システムごとの専用端末である場合が多かった。すなわち、従来のコンテンツ配信システムでは、たとえば、あらかじめサービスごとに「機器バインド」にするか「メディアバインド」にするかが決定されており、それを実現するための専用のシステムが構築されていた。ここで、機器バインドとは、指定された機器のみで使用可能なことであり、メディアバインドとは、指定されたメディアでのみ使用可能なことである。

【０００５】

【発明が解決しようとする課題】しかしながら、このような従来のコンテンツ配信システムにおいては、サービスごとに専用のシステムを構築していたため、同じシステムで異なるバインド方式によるコンテンツ配信サービスを行うことができず、また、サービスやコンテンツ、端末に応じてサーバが自由にバインド方式を設定することができなかった。すなわち、同じ枠組み（システム）でコンテンツ配信のいろいろなサービスを行うことができなかった。

【０００６】本発明は、かかる点に鑑みてなされたものであり、同じ枠組みでコンテンツ配信のいろいろなサービスを行うことができるコンテンツ配信システムを提供することを目的とする。

【０００７】

【課題を解決するための手段】（１）本発明のコンテンツ配信システムは、コンテンツを配信するサーバ装置と、前記サーバ装置によって配信されたコンテンツを記録する記録媒体装置と、前記記録媒体装置に記録されたコンテンツを再生する再生装置とを有するコンテンツ配信システムであって、前記記録媒体装置は、複数の記録媒体装置用の鍵を記憶する第１記憶手段、を有し、前記再生装置は、複数の再生装置用の鍵を記憶する第２記憶手段、を有し、前記サーバ装置は、前記第１記憶手段に記憶された複数の記録媒体装置用の鍵とおのおの対をなす複数の記録媒体装置用の鍵および前記第２記憶手段に記憶された複数の再生装置用の鍵とおのおの対をなす複数の再生装置用の鍵の中からそれぞれ１つの記録媒体装置用の鍵および再生装置用の鍵を取得する取得手段と、前記取得手段によって取得された記録媒体装置用の鍵および再生装置用の鍵を用いて、暗号化されたコンテンツを復号化するための暗号化コンテンツ復号鍵を二重に暗号化する暗号化手段と、を有する構成を採る。

【０００８】この構成によれば、記録媒体装置に複数の鍵を格納するとともに再生装置に複数の鍵を格納しておき、サーバ装置で、暗号化コンテンツ復号鍵を、記録媒体装置の鍵と再生装置の鍵とで二重に暗号化するため、同じ枠組みでバインド方式を自由に制御することができ、同じ枠組みでコンテンツ配信のいろいろなサービスを行うことができる。

【０００９】（２）本発明のコンテンツ配信システムは、上記構成において、前記第１記憶手段に記憶された複数の記録媒体装置用の鍵は、全部の記録媒体装置に共有の全共有鍵と、各記録媒体装置に固有の固有鍵とを含む構成を採る。

【００１０】この構成によれば、複数の記録媒体装置用の鍵は、少なくとも、全共有鍵と、固有鍵とを含むため、全共有レベルと固有レベルとを自由に設定することができる。

【００１１】（３）本発明のコンテンツ配信システムは、上記構成において、前記第１記憶手段に記憶された複数の記録媒体装置用の鍵は、全部の記録媒体装置に共有の全共有鍵と、特定の範囲の記録媒体装置に共有の特定範囲共有鍵とを含む構成を採る。

【００１２】この構成によれば、複数の記録媒体装置用の鍵は、少なくとも、全共有鍵と、特定範囲共有鍵とを含むため、全共有レベルと特定範囲共有レベルとを自由に設定することができる。

【００１３】（４）本発明のコンテンツ配信システムは、上記構成において、前記第１記憶手段に記憶された複数の記録媒体装置用の鍵は、各記録媒体装置に固有の固有鍵と、特定の範囲の記録媒体装置に共有の特定範囲共有鍵とを含む構成を採る。

【００１４】この構成によれば、複数の記録媒体装置用の鍵は、少なくとも、固有鍵と、特定範囲共有鍵とを含むため、固有レベルと特定範囲共有レベルとを自由に設定することができる。

【００１５】（５）本発明のコンテンツ配信システムは、上記構成において、前記第１記憶手段に記憶された複数の記録媒体装置用の鍵は、全部の記録媒体装置に共有の全共有鍵と、各記録媒体装置に固有の固有鍵と、特定の範囲の記録媒体装置に共有の特定範囲共有鍵とを含む構成を採る。

【００１６】この構成によれば、複数の記録媒体装置用の鍵は、少なくとも、全共有鍵と、固有鍵と、特定範囲共有鍵とを含むため、全共有レベルと固有レベルと特定範囲共有レベルとを自由に設定することができる。

【００１７】（６）本発明のコンテンツ配信システムは、上記構成において、前記第２記憶手段に記憶された複数の再生装置用の鍵は、全部の再生装置に共有の全共有鍵と、各再生装置に固有の固有鍵とを含む構成を採る。

【００１８】この構成によれば、複数の再生装置用の鍵は、少なくとも、全共有鍵と、固有鍵とを含むため、全共有レベルと固有レベルとを自由に設定することができる。

【００１９】（７）本発明のコンテンツ配信システムは、上記構成において、前記第２記憶手段に記憶された複数の再生装置用の鍵は、全部の再生装置に共有の全共有鍵と、特定の範囲の再生装置に共有の特定範囲共有鍵とを含む構成を採る。

【００２０】この構成によれば、複数の再生装置用の鍵は、少なくとも、全共有鍵と、特定範囲共有鍵とを含むため、全共有レベルと特定範囲共有レベルとを自由に設定することができる。

【００２１】（８）本発明のコンテンツ配信システムは、上記構成において、前記第２記憶手段に記憶された複数の再生装置用の鍵は、各再生装置に固有の固有鍵と、特定の範囲の再生装置に共有の特定範囲共有鍵とを含む構成を採る。

【００２２】この構成によれば、複数の再生装置用の鍵は、少なくとも、固有鍵と、特定範囲共有鍵とを含むため、固有レベルと特定範囲共有レベルとを自由に設定することができる。

【００２３】（９）本発明のコンテンツ配信システムは、上記構成において、前記第２記憶手段に記憶された複数の再生装置用の鍵は、全部の再生装置に共有の全共有鍵と、各再生装置に固有の固有鍵と、特定の範囲の再生装置に共有の特定範囲共有鍵とを含む構成を採る。

【００２４】この構成によれば、複数の再生装置用の鍵は、少なくとも、全共有鍵と、固有鍵と、特定範囲共有鍵とを含むため、全共有レベルと固有レベルと特定範囲共有レベルとを自由に設定することができる。

【００２５】（１０）本発明のコンテンツ配信システムは、上記構成において、前記サーバ装置は、暗号化コンテンツ復号鍵を二重に暗号化する際に使用する記録媒体装置用の鍵および再生装置用の鍵を、コンテンツ配信サービスに応じて決定する決定手段、をさらに有し、前記取得手段は、前記決定手段の決定結果に従って、前記第１記憶手段に記憶された複数の記録媒体装置用の鍵とおのおの対をなす複数の記録媒体装置用の鍵および前記第２記憶手段に記憶された複数の再生装置用の鍵とおのおの対をなす複数の再生装置用の鍵の中からそれぞれ１つの記録媒体装置用の鍵および再生装置用の鍵を取得する、構成を採る。

【００２６】この構成によれば、暗号化コンテンツ復号鍵を二重に暗号化する際に使用する記録媒体装置用の鍵および再生装置用の鍵を、コンテンツ配信サービスに応じて決定するため、同じ枠組みでバインド方式をサービスに応じて自由に制御することができる。

【００２７】（１１）本発明のコンテンツ配信システムは、上記構成において、前記サーバ装置は、前記暗号化手段によって二重に暗号化された暗号化コンテンツ復号鍵ならびに当該暗号化コンテンツ復号鍵を二重に暗号化する際に使用した記録媒体装置用の鍵および再生装置用の鍵に関する暗号化コンテンツ復号鍵暗号化情報を配信する配信手段、をさらに有する構成を採る。

【００２８】この構成によれば、暗号化コンテンツ復号鍵暗号化情報を配信するため、クライアント側では二重暗号化に使用された鍵を容易に知ることができる。

【００２９】（１２）本発明の、コンテンツ配信システムにおけるバインド方式制御方法は、コンテンツを配信するサーバ装置と、前記サーバ装置によって配信されたコンテンツを記録する記録媒体装置と、前記記録媒体装置に記録されたコンテンツを再生する再生装置とを有するコンテンツ配信システムにおけるバインド方式制御方法であって、前記サーバ装置が、前記記録媒体装置に記憶された複数の記録媒体装置用の鍵とおのおの対をなす複数の記録媒体装置用の鍵および前記再生装置に記憶された複数の再生装置用の鍵とおのおの対をなす複数の再生装置用の鍵の中からそれぞれ１つの記録媒体装置用の鍵および再生装置用の鍵を取得する取得ステップと、前記サーバ装置が、前記取得ステップで取得した記録媒体装置用の鍵および再生装置用の鍵を用いて、暗号化されたコンテンツを復号化するための暗号化コンテンツ復号鍵を二重に暗号化する暗号化ステップと、を有するようにした。

【００３０】この方法によれば、記録媒体装置に複数の鍵を格納するとともに再生装置に複数の鍵を格納しておき、サーバ装置で、暗号化コンテンツ復号鍵を、記録媒体装置の鍵と再生装置の鍵とで二重に暗号化するため、同じ枠組みでバインド方式を自由に制御することができ、同じ枠組みでコンテンツ配信のいろいろなサービスを行うことができる。

【００３１】（１３）本発明のサーバ装置は、コンテンツを配信するサーバ装置であって、前記サーバ装置によって配信されたコンテンツを記録する記録媒体装置に記憶された複数の記録媒体装置用の鍵とおのおの対をなす複数の記録媒体装置の鍵および前記記録媒体装置に記録されたコンテンツを再生する再生装置に記憶された複数の再生装置用の鍵とおのおの対をなす複数の再生装置用の鍵の中からそれぞれ１つの記録媒体装置用の鍵および再生装置用の鍵を取得する取得手段と、前記取得手段によって取得された記録媒体装置用の鍵および再生装置用の鍵を用いて、暗号化されたコンテンツを復号化するための暗号化コンテンツ復号鍵を二重に暗号化する暗号化手段と、を有する構成を採る。

【００３２】この構成によれば、上記のコンテンツ配信システムを構築するための一要素であるサーバ装置を提供することができる。

【００３３】（１４）本発明の、サーバ装置におけるバインド方式制御方法は、コンテンツを配信するサーバ装置におけるバインド方式制御方法であって、前記サーバ装置によって配信されたコンテンツを記録する記録媒体装置に記憶された複数の記録媒体装置用の鍵とおのおの対をなす複数の記録媒体装置用の鍵および前記記録媒体装置に記録されたコンテンツを再生する再生装置に記憶された複数の再生装置用の鍵とおのおの対をなす複数の再生装置用の鍵の中からそれぞれ１つの記録媒体装置用の鍵および再生装置用の鍵を取得する取得ステップと、前記取得ステップで取得した記録媒体装置用の鍵および

再生装置用の鍵を用いて、暗号化されたコンテンツを復号化するための暗号化コンテンツ復号鍵を二重に暗号化する暗号化ステップと、を有するようにした。

【００３４】この方法によれば、上記のコンテンツ配信システムを構築するための一要素であるサーバ装置におけるバインド方式制御方法を提供することができる。

【００３５】（１５）本発明の、サーバ装置におけるバインド方式制御プログラムは、コンテンツを配信するサーバ装置におけるバインド方式制御プログラムであって、前記サーバ装置によって配信されたコンテンツを記録する記録媒体装置に記憶された複数の記録媒体装置用の鍵とおのおの対をなす複数の記録媒体装置用の鍵および前記記録媒体装置に記録されたコンテンツを再生する再生装置に記憶された複数の再生装置用の鍵とおのおの対をなす複数の再生装置用の鍵の中からそれぞれ１つの記録媒体装置用の鍵および再生装置用の鍵を取得する取得ステップと、前記取得ステップで取得した記録媒体装置用の鍵および再生装置用の鍵を用いて、暗号化されたコンテンツを復号化するための暗号化コンテンツ復号鍵を二重に暗号化する暗号化ステップと、をコンピュータに実行させるようにした。

【００３６】このプログラムによれば、上記のコンテンツ配信システムを構築するための一要素であるサーバ装置におけるバインド方式制御プログラムを提供することができる。

【００３７】（１６）本発明の記録媒体装置は、サーバ装置によって配信されたコンテンツを記録する記録媒体装置であって、複数の記録媒体装置用の鍵を記憶する第１記憶手段、を有する構成を採る。

【００３８】この構成によれば、上記のコンテンツ配信システムを構築するための一要素である記録媒体装置を提供することができる。

【００３９】（１７）本発明の再生装置は、サーバ装置によって配信され記録媒体装置に記録されたコンテンツを再生する再生装置であって、複数の再生装置用の鍵を記憶する第２記憶手段、を有する構成を採る。

【００４０】この構成によれば、上記のコンテンツ配信システムを構築するための一要素である再生装置を提供することができる。

【００４１】（１８）本発明のコンテンツ配信システムは、コンテンツを配信するサーバ装置と、前記サーバ装置によって配信されたコンテンツを記録する記録媒体装置と、前記記録媒体装置に記録されたコンテンツを再生する再生装置とを有するコンテンツ配信システムであって、前記記録媒体装置は、複数の記録媒体装置用の鍵を記憶する第１記憶手段、を有し、前記再生装置は、複数の再生装置用の鍵を記憶する第２記憶手段、を有し、前記サーバ装置は、前記第１記憶手段に記憶された複数の記録媒体装置用の鍵とおのおの対をなす複数の記録媒体装置用の鍵および前記第２記憶手段に記憶された複数の再生装置用の鍵とおのおの対をなす複数の再生装置用の鍵の中からそれぞれ１つの記録媒体装置用の鍵および再生装置用の鍵を取得する取得手段と、前記取得手段によって取得された記録媒体装置用の鍵および再生装置用の鍵を用いて、配信するコンテンツを二重に暗号化する暗号化手段と、を有する構成を採る。

【００４２】この構成によれば、記録媒体装置に複数の鍵を格納するとともに再生装置に複数の鍵を格納しておき、サーバ装置で、配信するコンテンツを、記録媒体装置の鍵と再生装置の鍵とで二重に暗号化するため、同じ枠組みでバインド方式を自由に制御することができ、同じ枠組みでコンテンツ配信のいろいろなサービスを行うことができる。

【００４３】

【発明の実施の形態】本発明の骨子は、たとえば、データの暗号化方式として公開鍵暗号方式を例にとると、あらかじめ記録媒体装置に複数の秘密鍵を格納するとともに再生装置に複数の秘密鍵を格納しておき、サーバ装置で、サービスに応じて、暗号化コンテンツの復号鍵を記録媒体装置の公開鍵と再生装置の公開鍵とで二重に暗号化することにより、同じ枠組み（システム）でバインド方式を自由に制御できるようにすることである。

【００４４】以下、本発明の実施の形態について、図面を参照して詳細に説明する。なお、ここでは、データの暗号化方式として公開鍵暗号方式を例にとって説明する。また、コンテンツ配信システムとして、配信されるコンテンツが音楽の場合（音楽配信システム）を例にとって説明する。

【００４５】図１は、本発明の一実施の形態に係るコンテンツ配信システムのサーバ側の構成を主として示すブロック図、図２は、同コンテンツ配信システムのクライアント（蓄積・再生）側の構成を示すブロック図である。

【００４６】図１に示すサーバ（サーバ装置）１００は、コンテンツ管理部１１０、コンテンツ鍵管理領域１２０、コンテンツ暗号化部１３０、暗号化コンテンツ管理領域１４０、認証部１５０、公開鍵取得部１６０、コンテンツ復号鍵二重暗号化部１７０、ライセンスデータ作成部１８０、およびライセンスデータ配信部１９０を有する。

【００４７】一方、クライアント側は、大別して、図２に示すように、セキュアデバイス（記録媒体装置）２００、ライセンス処理アプリケーションソフトウエア（以下単に「ライセンス処理アプリ」という）（再生処理装置）３００、デコーダインタフェース（Ｉ／Ｆ）ライブラリ（再生装置）４００、およびオーディオデコーダ（再生装置）５００を有する。

【００４８】なお、本実施の形態では、再生処理装置と再生装置は、別の機器であるが、これに限定されるわけではなく、同じ機器であってもよい。また、記録媒体装

置は、取り外し可能な記録媒体（メディア）であっても再生処置装置と同じ機器であってもよい。

【００４９】コンテンツ管理部１１０は、いろいろな配信用コンテンツ（たとえば、音楽、映画、電子書籍、ゲームプログラム、電子チケットなど）を格納し管理する。コンテンツ鍵管理領域１２０は、コンテンツを暗号化・復号化するための鍵（コンテンツ鍵）を管理する。配信するコンテンツは、コンテンツ暗号化部１３０で、コンテンツ鍵を用いて暗号化される。暗号化されたコンテンツは、暗号化コンテンツ管理領域１４０に格納され管理される。なお、コンテンツ鍵は、コンテンツの暗号化に使用される場合は、コンテンツ暗号鍵と呼ばれ、暗号化コンテンツの復号化に使用する場合は暗号化コンテンツ復号鍵（以下単に「コンテンツ復号鍵」という）と呼ばれる。

【００５０】認証部１５０は、認証処理を行う。具体的には、クライアント側（コンテンツ配信先）と相互認証を行い、セキュアセッションを張る。セキュアセッションが張られると、公開鍵取得部１６０は、上記コンテンツ鍵を暗号化するための公開鍵を取得する。具体的には、公開鍵取得部１６０は、コンテンツ復号鍵を二重に暗号化するために、２種類の公開鍵、たとえば、セキュアデバイスの公開鍵とデコーダの公開鍵を取得する。後で詳述するように、セキュアデバイスの公開鍵は複数存在し、デコーダの公開鍵も複数存在している。複数存在する公開鍵のうちのどの公開鍵を使用するかは、サーバ１００が、サービスに応じて決定する。公開鍵取得のタイミングは、たとえば、クライアント側からサーバ１００にライセンス要求が届いた時に、上記のセキュアセッションを張って取得する。

【００５１】コンテンツ復号鍵二重暗号化部１７０は、公開鍵取得部１６０によって取得された２種類の公開鍵（セキュアデバイスの公開鍵とデコーダの公開鍵）を用いてコンテンツ復号鍵を二重に暗号化する。後で詳述するが、セキュアデバイスの公開鍵に関しては、セキュアデバイスごとに異なる鍵を使用するとメディアバインドにすることができ、デコーダの公開鍵に関しては、デコーダごとに異なる鍵を使用すると機器バインドにすることができる。二重に暗号化されたコンテンツ復号鍵は、セキュアデバイスの公開鍵による暗号化については、セキュアデバイスと相互認証したライセンス処理アプリで復号化され、デコーダの公開鍵による暗号化については、デコーダの内部で復号化される。

【００５２】ライセンスデータ作成部１８０は、ライセンスデータの作成を行う。ライセンスデータの一例は、たとえば、図３に示すとおりである。図３に示すライセンスデータ２６０は、ライセンスＩＤ、コンテンツＩＤ、コンテンツ関連情報、および利用規則（Usage Rule）に加えて、コンテンツ復号鍵暗号化情報２７０と、セキュアデバイスの公開鍵２８０とデコーダの公開鍵２８５を用いて二重に暗号化されたコンテンツ復号鍵２９０とを含み、デジタル署名されている。コンテンツ関連情報は、コンテンツが音楽の場合、たとえば、曲名やアーティスト名などである。利用規則には、静的プロパティ（Static Properties）と動的プロパティ（Variable Properties）とがあり、前者は、たとえば、再生期限などであり、後者は、たとえば、再生回数や総再生時間などである。また、コンテンツ復号鍵暗号化情報２７０は、コンテンツ復号鍵の二重暗号化に使用した鍵（セキュアデバイスの公開鍵２８０とデコーダの公開鍵２８５）の情報であり、たとえば、数ビットのフラグ、鍵のハッシュ、証明書などを利用したものである。

【００５３】ライセンスデータ配信部１９０は、ライセンスデータ作成部１８０で作成されたライセンスデータ２６０をクライアント側に配信する。

【００５４】次に、クライアント側の構成について詳細に説明する。

【００５５】セキュアデバイス２００は、たとえば、カード型の記録媒体（メディア）であって、ＴＲＭ（耐タンパモジュール）２１０とフラッシュメモリ２５０を内蔵している。

【００５６】ＴＲＭ２１０は、署名機能を行う署名部２２０と、セキュアデバイス証明書格納領域２３０と、セキュアデバイス秘密鍵格納領域２４０とを有する。セキュアデバイス秘密鍵格納領域２４０には、複数の秘密鍵、ここでは、たとえば、セキュアデバイス共有秘密鍵（全共有鍵）２４１、セキュアデバイス固有秘密鍵（固有鍵）２４２、およびサービス利用者鍵（特定範囲共有鍵）２４３の３つの秘密鍵が格納されている。なお、ＴＲＭ２１０内の秘密鍵（セキュアデバイス共有秘密鍵２４１、セキュアデバイス固有秘密鍵２４２、サービス利用者鍵２４３）へは、ＴＲＭ２１０内部（たとえば、署名部２２０）からしかアクセスすることができない。また、ＴＲＭ２１０内部の機能（たとえば、署名部２２０）へは、たとえば相互認証により、正当性が確認されたアプリケーションソフトウエアしかアクセスすることができない。

【００５７】ここで、セキュアデバイス共有秘密鍵２４１とは、全セキュアデバイス（メディア）に共有の秘密鍵であり、セキュアデバイス固有秘密鍵２４２とは、各セキュアデバイス（メディア）に固有の秘密鍵であり、サービス利用者鍵２４３とは、特定サービス（たとえば、Ａ社の音楽配信サービス）の会員が持っているセキュアデバイス（メディア）に共有の秘密鍵である。

【００５８】フラッシュメモリ２５０には、サーバ１００から配信されたライセンスデータ２６０が格納されている。ライセンスデータ２６０には、上記のように、セキュアデバイス（メディア）の公開鍵２８０とデコーダの公開鍵２８５とで二重に暗号化されたコンテンツ復号鍵２９０と、二重暗号化に際して使用した鍵の情報であ

るコンテンツ復号鍵暗号化情報２７０とが格納されている。

【００５９】なお、セキュアデバイス２００が取り外し可能な記録媒体（メディア）である場合、セキュアデバイス２００を装着する機器は、特に限定されない。たとえば、携帯電話でも携帯端末（ＰＤＣ）でもパソコンでもよく、ＴＲＭを内蔵したメディアに対応したスロットがついていればよい。

【００６０】ライセンス処理アプリ３００は、ライセンス処理を行うためのアプリケーションソフトウエアであって、たとえば、図１に示すように、認証部３１０、公開鍵格納領域３２０、ライセンスデータ取得部３３０、コンテンツ復号鍵暗号化情報判定部３４０、およびコンテンツ復号鍵復号化部３５０を有する。

【００６１】認証部３１０は、サーバ１００にライセンス要求を出すときに、サーバ１００と相互認証を行い、セキュアセッションを張る。

【００６２】公開鍵格納領域３２０には、セキュアデバイス２００の公開鍵とデコーダ５００の公開鍵が格納されている。セキュアデバイス２００の公開鍵には、セキュアデバイス共有秘密鍵２４１と対をなす公開鍵、セキュアデバイス固有秘密鍵２４２と対をなす公開鍵、およびサービス利用者鍵２４３と対をなす公開鍵が含まれている。また、デコーダ５００の公開鍵には、後述するオーディオ共有秘密鍵５１、オーディオ固有秘密鍵５１２、およびメーカ固有鍵５１３とおのおの対をなす公開鍵が含まれている。

【００６３】なお、本実施の形態では、公開鍵格納領域３２０はライセンス処理アプリ３００に設けられているが、これに限定されるわけではなく、端末にあってもセキュアデバイスにあってもよい。

【００６４】ライセンスデータ取得部３３０は、サーバ１００から配信されたライセンスデータ２６０を取得する。コンテンツ復号鍵暗号化情報判定部３４０は、ライセンスデータ取得部３３０で取得されたライセンスデータ２６０からコンテンツ復号鍵暗号化情報２７０を取り出して、コンテンツ復号鍵を暗号化する際に使用された鍵がどれであるかを判定する。コンテンツ復号鍵復号化部３５０は、コンテンツ復号鍵暗号化情報判定部３４０の判定結果に従って、たとえば、セキュアデバイス秘密鍵格納領域２４０からその判定結果に対応するセキュアデバイス秘密鍵を読み出し、読み出した鍵を用いてコンテンツ復号鍵の復号化（第１回目）を行う。なお、復号化（第１回目）されたコンテンツ復号鍵は、後述する場合と同様に、デコーダに送られ、デコーダの内部で完全に復号化（第２回目）される。

【００６５】デコーダインタフェースライブラリ４００は、オーディオデコーダ５００とライセンス処理アプリ３００との中継を行う。

【００６６】オーディオデコーダ５００は、図２に示すように、デコーダ秘密鍵格納領域５１０と、コンテンツ復号鍵復号化部５２０とを有する。

【００６７】デコーダ秘密鍵格納領域５１０には、複数の秘密鍵、ここでは、たとえば、オーディオ共有秘密鍵（全共有鍵）５１１、オーディオ固有秘密鍵（固有鍵）５１２、およびメーカ固有鍵（特定範囲共有鍵）２４３の３つの秘密鍵が格納されている。ここで、オーディオ共有秘密鍵５１１とは、全オーディオデコーダに共有の秘密鍵であり、オーディオ固有秘密鍵５１２とは、各オーディオデコーダに固有の秘密鍵であり、メーカ固有鍵５１３とは、メーカごとに共有の秘密鍵である。

【００６８】コンテンツ復号鍵復号化部５２０は、ライセンス処理アプリ３００内のコンテンツ復号鍵暗号化情報判定部３４０の判定結果に従って、デコーダ秘密鍵格納領域５１０からその判定結果に対応するデコーダ秘密鍵を読み出し、読み出した鍵を用いてコンテンツ復号鍵の復号化（第２回目）を行う。この段階で、二重に暗号化されていたコンテンツ復号鍵２９０は、完全に復号化される。

【００６９】次いで、サーバ１００で二重に暗号化された後サーバ１００から配信されセキュアデバイス２００に格納された二重暗号化コンテンツ復号鍵２９０を復号化する際の手順について、図２を用いて説明する。

【００７０】セキュアデバイス２００とライセンス処理アプリ３００との間で相互認証を行った後、まず、ライセンス処理アプリ３００が、セキュアデバイス２００内のフラッシュメモリ２５０からライセンスデータ２６０を読み出す（①）。

【００７１】そして、コンテンツ復号鍵暗号化情報判定部３４０で、読み出したライセンスデータ２６０からコンテンツ復号鍵暗号化情報２７０を取り出して、コンテンツ復号鍵２９０を暗号化する際に使用された鍵がどれであるかを判定する（②）。この判定結果は、セキュアデバイス２００内のＴＲＭ２１０に送られるとともに、デコーダインタフェースライブラリ４００を経由してオーディオデコーダ５００に送られる。

【００７２】そして、コンテンツ復号鍵復号化部３５０で、ＴＲＭ２１０内のセキュアデバイス秘密鍵格納領域２４０からコンテンツ復号鍵暗号化情報判定部３４０の判定結果に対応するセキュアデバイス秘密鍵を読み出し、読み出した鍵を用いてコンテンツ復号鍵２９０の復号化（第１回目）を行う（③）。

【００７３】その後、セキュアデバイス２００の鍵で復号化（第１回目）されたコンテンツ復号鍵２９０は、デコーダインタフェースライブラリ４００を経由して、オーディオデコーダ５００内のコンテンツ復号鍵復号化部５２０に送信される（④）。

【００７４】そして、オーディオデコーダ５００内のコンテンツ復号鍵復号化部５２０で、デコーダ秘密鍵格納領域５１０からライセンス処理アプリ３００内のコンテ

ンツ復号鍵暗号化情報判定部３４０の判定結果に対応するデコーダ秘密鍵を読み出し、読み出した鍵を用いてコンテンツ復号鍵２９０の復号化（第２回目）を行う（ⓑ）。これにより、二重に暗号化されていたコンテンツ復号鍵２９０は、完全に復号化され、暗号化コンテンツの復号化に使用される。

【００７５】なお、デコーダ秘密鍵格納領域５１０は、デコーダインタフェースライブラリ４００にあってもよい。また、ライセンス処理アプリ３００で行う処理（コンテンツ復号鍵の復号化）は、ＴＲＭ２１０内で行うようにしてもよい。また、ＴＲＭ２１０やフラッシュメモリ２５０の存在場所は、セキュアデバイス（カード）２００に限定されるわけではなく、端末にあってもよい。

【００７６】次いで、上記構成を有するコンテンツ配信システムがもたらす効果について、図４を用いて具体的に説明する。図４は、記憶媒体装置（メディア）の鍵と再生装置（デコーダ）の鍵の各種組合せにより暗号化した場合に考えられるサービスを示した図である。

【００７７】ここで、メディア共有鍵は、全メディアに共通に入っている鍵である（たとえば、セキュアデバイス共有秘密鍵２４１）。この鍵を使用した場合、どのメディアでも再生可能であるが、暗号を全くかけない場合と異なり、セキュアデバイスと相互認証をした信頼できるアプリケーションソフトウエアからならどの機器でも復号化できるが、信頼できないアプリケーションソフトウエアでは復号化できないため、復号化後のデータを抜き取られるおそれがない。

【００７８】メディア固有鍵は、メディアごとに異なる、各メディア唯一の鍵であって、メディアとメディア固有鍵とが１対１で対応付けられている（たとえば、セキュアデバイス固有秘密鍵２４２）。この鍵を使用した場合、特定メディアでのみ再生可能であり、メディアからデータを抜き出すと意味のないデータになるため、他のメディアにコピーされるおそれがない。

【００７９】サービス利用者鍵は、特定サービス（たとえば、Ａ社の音楽配信サービス）の会員が持っているメディアに共通に入っている鍵である（たとえば、サービス利用者鍵２４３）。この鍵を使用した場合、サービス利用者のメディアでのみ再生可能である。

【００８０】デコーダ共有鍵は、このシステムのデコーダ全部に共通に入っている鍵である（たとえば、オーディオ共有秘密鍵５１１）。この鍵を使用した場合、どのデコーダでも再生可能であるが、暗号を全くかけない場合と異なり、このシステムにのっとらないデコーダ（特に違法デコーダなど）では再生できない。

【００８１】デコーダ固有鍵は、デコーダごとに異なる、各デコーダ唯一の鍵であって、デコーダとデコーダ固有鍵とが１対１で対応付けられる（たとえば、オーディオ固有秘密鍵５１２）。この鍵を使用した場合、特定デコーダでのみ再生可能であり、他のデコーダに持って行っても意味のないデータになるため、抜き出されて使用されるおそれがない。

【００８２】メーカ固有鍵は、特定メーカのデコーダに共通に入っている鍵である（たとえば、メーカ固有鍵５１３）。この鍵を使用した場合、特定メーカの機器で再生可能である。

【００８３】なお、鍵の種類は、上記の例に限定されない。たとえば、メディアの特性範囲共有鍵としては、サービス利用者鍵のほかに、特定メーカのメディアに入っている鍵、特定バージョンのメディアに入っている鍵なども考えられる。

【００８４】上記の鍵を利用してコンテンツ復号鍵を二重に暗号化すると、その組合せに応じて、同じ枠組みでコンテンツ配信のいろいろなサービスを行うことができる（図中Ａ～Ｉ参照）。

【００８５】１）メディア共有鍵とデコーダ共有鍵を利用した場合（図中Ａの場合）
どのメディア、どのデコーダに持って行っても再生可能である。ただし、抜き出して本システム以外で使用することはできない。すなわち、正しいアプリケーションソフトウエア、デコーダでの使用ならばフリーである。具体例としては、お試し版、プロモーション用の場合である。

【００８６】２）メディア固有鍵とデコーダ共有鍵を利用した場合（図中Ｂの場合）
メディアバインドになり、ダウンロード時のメディアでのみ再生可能である。この場合、デコーダはどれでもよい。具体例としては、レンタルの場合である。

【００８７】３）サービス利用者鍵とデコーダ共有鍵を利用した場合（図中Ｃの場合）
サービス利用者のメディアであればどの機器でも再生可能である。また、サービス利用者間でコピー可能である。具体例としては、サービス利用者への無料配布の場合である。

【００８８】４）メディア共有鍵とデコーダ固有鍵を利用した場合（図中Ｄの場合）
機器バインドになり、どのメディアに持って行ってもよいが、再生できる機器は決まっており、メディアを盗んでも再生できない。具体例としては、視聴覚室、ミュージックカフェの場合である。

【００８９】５）メディア固有鍵とデコーダ固有鍵を利用した場合（図中Ｅの場合）
メディアバインドかつ機器バインドになり、ダウンロード時のメディアと機器でのみ再生可能である。他の機器に差しても、データを盗んでも、いずれも再生できない。具体例としては、個人利用（個人購入）の場合である。

【００９０】６）サービス利用者鍵とデコーダ固有鍵を利用した場合（図中Ｆの場合）
サービス利用者のメディアで、指定された機器であれば

再生可能である。具体例としては、サービス利用者への限定販売の場合である。

【００９１】７）メディア共有鍵とメーカ固有鍵を利用した場合（図中Ｇの場合）

特定メーカのデコーダであればどの機器でも再生可能である。また、同じメーカのデコーダを持っているユーザ間でコピー可能である。具体例としては、特定メーカのユーザ（デコーダ使用者）に無料配布する場合である。

【００９２】８）メディア固有鍵とメーカ固有鍵を利用した場合（図中Ｈの場合）

特定メーカのデコーダで、ダウンロード時のメディアであれば再生可能である。具体例としては、特定メーカのユーザ（デコーダ使用者）に限定販売する場合である。

【００９３】９）サービス利用者鍵とメーカ固有鍵を利用した場合（図中Ｉの場合）

サービス利用者のメディアで、かつ特定メーカのデコーダであれば再生可能である。また、同じサービス利用者でかつ同じメーカのユーザ（デコーダ利用者）間でコピー可能である。具体例としては、指定されたサービス・デコーダメーカのユーザに無料配布する場合である。

【００９４】なお、以下に、３つの比較例を示しておく。

【００９５】１０）デコーダの鍵は利用したがメディアの鍵での暗号化はない場合（図中Ｋの場合）

メディアのＴＲＭにアクセスする必要がなくなるため不正のアプリケーションソフトウエアでも利用できてしまう。たとえば、正当なアプリケーションソフトウエアで利用期間を制限しようとすると、違法なアプリケーションソフトウエアが作られてしまう。

【００９６】１１）メディアの鍵は利用したがデコーダの鍵での暗号化はない場合（図中Ｊの場合）

コンテンツ復号鍵がデコーダに渡る時に平文になっているため、そこで盗聴が行われると、本システム以外に持ち出して自由に利用できてしまう。すなわち、メディアの鍵で暗号化している意味もなくなってしまう。

【００９７】１２）メディアの鍵でもデコーダの鍵でも暗号化はない場合（図中Ｌの場合）

抜き出して本システム以外で利用できてしまう。違法なアプリケーションソフトウエアでも利用できる。すなわち、何の制限もなく、他システムでの利用もできてしまい、完全フリーの場合である。

【００９８】このように、本実施の形態によれば、セキュアデバイス２００に複数の秘密鍵を格納するとともにデコーダ５００に複数の秘密鍵を格納しておき、サーバ１００で、サービスに応じて、暗号化コンテンツの復号鍵２９０をセキュアデバイス２００の公開鍵とデコーダ５００の公開鍵とで二重に暗号化するため、同じ枠組みでバインド方式を自由に制御することができ、同じ枠組みでコンテンツ配信のいろいろなサービスを行うことができる。すなわち、サーバ側で機器バインドやメディアバインドを自由に設定することができ、また、逆に言えば、機器やメディアにバインドされたものもバインドされていないものも同じ枠組みで利用することができる。より具体的には、メディアバインド（図４中のＢの場合）、機器バインド（図４中のＤの場合）、メディア・機器バインド（図４中のＥの場合）など、限られたユーザに対してのみ有効になるようなコンテンツ配信をサービスに応じて行うことが可能になる。また、プロモーション用（図４中のＡの場合）、コンテンツ配信サービスの販促用特典版（図４中のＣの場合）、各メーカのデコーダの販促用特典版（図４中のＧの場合）など、条件を満たしているユーザ間での譲渡も可能になる。

【００９９】さらに言えば、このように、そのもの自身は本来無意味だった「全共有鍵」（たとえば、図４中のメディア共有鍵とデコーダ共有鍵）をパラメータの１つとしてあえて取り扱うことにより、同じ枠組み、具体的には、機器・メディアバインド方式に機器のみ／メディアのみバインド方式も組み込んだサービス・プラットフォームを容易に実現することができる。

【０１００】なお、本実施の形態では、暗号化方式として公開鍵暗号方式を例にとっているが、これに限定されるわけではなく、サーバ側とクライアント（蓄積・再生）側とで対をなす鍵を持っていればよく、サーバ側とクライアント側がお互いに同じ鍵を保有する秘密鍵暗号方式（共通鍵暗号方式とも呼ばれる）にも適用可能である。

【０１０１】また、本実施の形態では、暗号化コンテンツ復号鍵を二重に暗号化して配信する場合について説明したが、二重に暗号化して配信するデータは、暗号化コンテンツ復号鍵に限定されるわけでなく、コンテンツそのものであってもよい。すなわち、コンテンツのサイズが大きい場合は、暗号化や配信に要する処理が重たくなるが、たとえば、コンテンツのサイズが比較的小さい場合や、コンテンツの更新が頻繁に生じる場合は、コンテンツ（特に後者の場合はその更新によって生じる差分データ）を二重に暗号化して配信することも可能である。

【０１０２】

【発明の効果】以上説明したように、本発明によれば、同じ枠組みでコンテンツ配信のいろいろなサービスを行うことができる。

【図面の簡単な説明】

【図１】本発明の一実施の形態に係るコンテンツ配信システムのサーバ側の構成を主として示すブロック図

【図２】同コンテンツ配信システムのクライアント（蓄積・再生）側の構成を示すブロック図

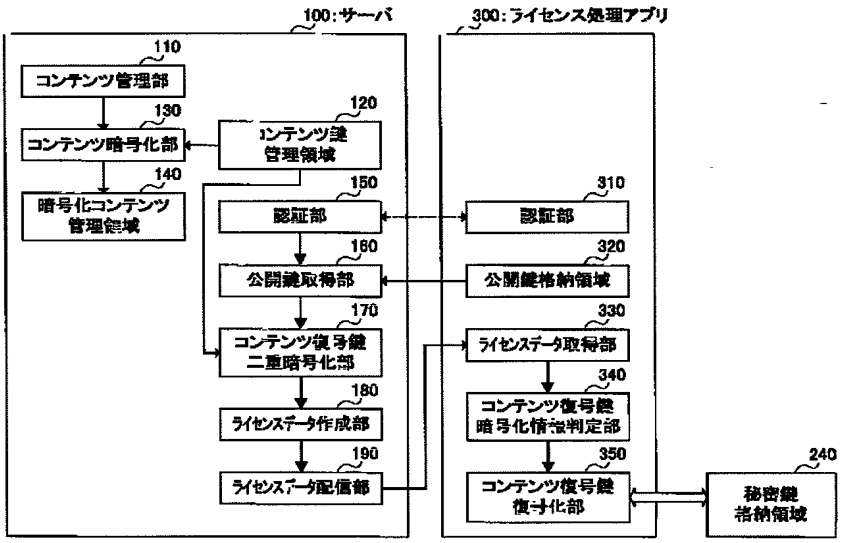
【図３】ライセンスデータの一例を示す図

【図４】記憶媒体装置（メディア）の鍵と再生装置（デコーダ）の鍵の各種組合せにより暗号化した場合に考えられるサービスを示した図

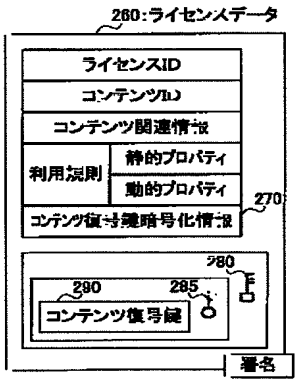
【符号の説明】

１００　サーバ
１６０　公開鍵取得部
１７０　コンテンツ復号鍵二重暗号化部
２００　セキュアデバイス
２４１　セキュアデバイス共有秘密鍵
２４２　セキュアデバイス固有秘密鍵
２４３　サービス利用者鍵
２５０　フラッシュメモリ
２７０　コンテンツ復号鍵暗号化情報
２８０　セキュアデバイスの鍵
２８５　デコーダの鍵
２９０　コンテンツ復号鍵
３００　ライセンス処理アプリ
３４０　コンテンツ復号鍵暗号化情報判定部
３５０、５２０　コンテンツ復号鍵復号化部
４００　デコーダインタフェースライブラリ
５００　オーディオデコーダ
５１１　オーディオ共有秘密鍵
５１２　オーディオ固有秘密鍵
５１３　メーカ固有鍵

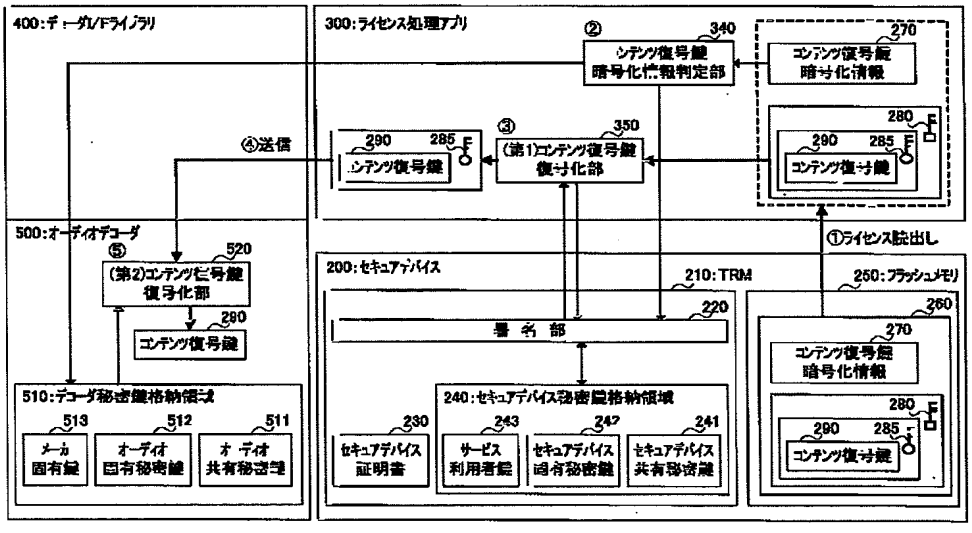
【図１】



【図３】



【図２】



【図4】

	メディア共有鍵	メディア固有鍵	サービス利用者鍵	メディアの鍵での暗号化なし
データ共有鍵	A お試し版・プロモーション用	B レンタル (メディアバインド)	C サービス利用者への無料配布	K
データ固有鍵	D 視聴覚室・ミュージックカフェ (機器バインド)	E 個人利用 (機器・メディアバインド)	F サービス利用者への限定販売	
メーカ固有鍵	G 特定メーカのユーザに無料配布	H 特定メーカのユーザに限定販売	I 指定サービス&デコーダメーカのユーザに無料配布	
データの鍵での暗号化なし	J			L

フロントページの続き

(51)Int.Cl.^{7}	識別記号	FI		(参考)
H04L 9/14		H04L 9/00	621A	

Fターム(参考) 5B017 AA07 BA07 CA16
5D044 AB02 AB05 AB07 DE50 GK17 HL11
5J104 AA12 EA04 EA17 EA20 MA05 NA02 NA27